The Different Motivations of Computer Attackers

BJ Bellamy

There are many common motivations for attacking information system. Some of these motivations are obvious, though most are not. And just as in the study of warfare, civil security architecture (such as bank design), and the work of the TSA, the design must be based on an understanding of the risks where risk is the combination of opportunity, ability, and *motivation*.

The general population is aware of some of the motivations that are behind information systems attacks. For example; personal gain, social activism (hacktavistism), and even state sponsored terrorism, warfare, and espionage. But there are other motivations that more often account for information system breaches. This ignorance of what motivates a cyber attack put us, the defenders, at a significant and unnecessary disadvantage and causes us to expend time and resources ineffectively.

The following are a few examples of the motivations that are behind many of the successful attacks we see in the news weekly.

Communications. If a system can be compromised, it can be used to send and receive communications anonymously. Steganography is the practice of hiding digital material within a digital file in such a way that the hidden material can be retrieved, but it cannot be detected without sophisticated digital analysis. For example, text or binary material such as an image can be hidden within a picture file without being detected simply by looking at the image. In fact, the size of the file containing the hidden material often does not change due to the inclusion of the hidden material.

Freedom. Another motivation is to *set information free*, which describes a commitment to the idea that all information should be freely available to everyone. The recent attacks in response to the death of Aaron Swartz illustrate both information breaches for the sole purpose of gathering information not available to the public so it can be posted openly, and cyber attacks against institutions simply because they had prosecuted Aaron Swartz for the intrusion. Another example is the wikileaks posting of military information.

Storage space. In other cases an intruder is looking for available disk space where they can store their files. This not only allows the attacker to avoid using their own disk space, but if the material is illegal or incriminating, storing it on a disk they do not own may afford some degree of protection from prosecution.

Processing power. Similar to storage space, an intruder often attacks a computer system simply to take advantage of the computing horse power that a compromised computer(s) can provide. A very common example of this is attacking hundreds and thousands of computers in order to gain remote control and turning them into bots, short for robot. A bot-master can then direct the computing horse power of any number of computers to crack passwords or mount a massive denial of service attack against a target.

Stepping stones. A successful computer attack is seldom targeted directly at a specific system. Organizations typically focus their information security efforts on protecting the servers that store their most sensitive information. Consequently, a direct frontal attack is the most difficult, and least likely to be successful. An attacker will instead attack a significantly less protected and monitored target such as the executive staff of the organization and their support staff. In some cases an organization's executive staff has excessive access to otherwise restricted information, and are less likely to be held to the same stringent controls and restrictions imposed on front-line staff.

Once one of these systems has been compromised, it can be used as a trusted internal system from which more invasive attacks can be launched. This stepping stone process can be used by an attacker to work their way throughout an organization until they get to the systems that contain information worth stealing or resources worth using.

The stepping stone motivation can extend beyond the initial organization into other organizations. For example, the actual target may be a highly protected federal system. Rather than attacking any of that network's components it would be easier, faster, and much more likely to succeed if you first attacked compromised a partner network such as a state agency that interfaces with the federal system. By gaining a toe-hold in the state agency's network, all activity directed towards the federal system would be seen as coming from an expected, and to some degree trusted, insider.

Distraction. Often and attacker will launch a Denial of Service (DoS) attack against one or more targets in order to draw attention away from the primary attack. With a digital smoke screen in place, an attacker's activity may go undetected long enough to take control of a system, plant malicious software, or gather protected data.

In conclusion, in describing some of the common, though not commonly recognized motivations for attacking information systems the point I want to make is that there are many obvious and not so obvious motivations for cyber attacks. And without this insight we will likely make mistakes regarding what we protect, how we protect it, and who/what we are protecting if from.